1 Executive Security Assessment Report

1.1 Introduction

This report outlines the findings from a security assessment conducted on the domain **dqbc.firstdataclients.co** The assessment was performed using a certified web application and infrastructure penetration testing tool, adhering to OWASP and OSCP methodologies. The analysis commenced on **October 5th** at **17:00** and concluded in **00h:13m:39s**. The tracking ID for this assessment is **10e88a40fa31**, and the scope included a basic analysis of the domain to identify potential security vulnerabilities.

1.2 Summary of Findings

The security assessment identified a total of **18** issues, categorized as **0** High, **1** Medium, **2** Low, and **15** informational. The most critical finding is the presence of an open HTTP port (**80**) without encryption, posing a Medium risk due to potential data interception, which requires immediate review for HTTPS redirection or HSTS implementation. Additionally, the SSL/TLS analysis revealed the use of TLS **1.2**, which is acceptable but lacks the enhanced security of TLS **1.3**. The Low-risk findings include a login form detection, which is within normal limits, and no outdated SSL protocols were found. The assessment also confirmed no shared hosting environments or brute-force vulnerable services, indicating a generally secure infrastructure. Immediate actions should focus on securing the HTTP service and considering an upgrade to TLS **1.3** for improved security.

1.3 Issues Table

Title	Risk
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security	Low
Login Form Detection Analysis	Low

1.4 Detailed Findings

1.4.1 Nmap Port Scan Results Analysis

Description:
The assessment identified an open HTTP port (**80**) on IP **107.162.144.175** without encryption, posing a Medium risk. This lack of encryption can lead to potential data interception by malicious actors.

Affected Assets:
- IP: **107.162.144.175** - Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations:
It is recommended to implement HTTPS redirection or enable HTTP Strict Transport Security (HSTS) to ensure encrypted communication over port **80**. This will mitigate the risk of data interception and enhance overall security posture.

1.4.2 SSL/TLS Protocols Security Assessment

Description:
The SSL/TLS analysis revealed that the endpoint is using TLS **1.2**, which is currently acceptable but does not provide the enhanced security features available in TLS **1.3**.

Affected Assets:
- **1** endpoint using TLS **1.2**

Recommendations:
Consider upgrading to TLS **1.3** to leverage improved security and performance benefits. This upgrade will align with current best practices and enhance cryptographic strength.

1.4.3 Login Form Detection Analysis

Description:
A single login form was detected across the application, which is within normal limits and poses a Low risk.

Affected Assets:
- URLs: - `https://dqbc.firstdataclients.com:443` - `http://dqbc.firstdataclients.com:80`

Recommendations:
Ensure that the login form is protected against common web vulnerabilities such as SQL injection and cross-site scripting (XSS). Implementing multi-factor authentication (MFA) can further secure user authentication processes.

1.5 General Recommendations

To enhance the overall security posture, it is recommended to prioritize securing HTTP services by implementing HTTPS redirection or HSTS, and consider upgrading to TLS **1.3** for improved cryptographic strength. Regular security assessments should be conducted to identify and mitigate emerging threats promptly.